CISCO SYSTEMS

Extensible Authentication Protocol Transport Layer Security
Deployment Guide for Wireless LAN Networks

1 Scope

This document discusses the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication protocol deployment in wireless networks. It introduces the EAP-TLS architecture and then discusses deployment issues. An example enterprise rollout for EAP-TLS is discussed in the section "Validation Lab" (Section 6).

2 Background

In September 1999, the IEEE approved the 802.11b (2.4-gigahertz [GHz] range, 11-Mbps throughput) and 802.11a (5-GHz range, 54-Mbps throughput) extensions. Since then, adoption of wireless LAN (WLAN) solutions in vertical (retail, education, health care, transportation, and so on) and horizontal markets has accelerated. As standardized by the IEEE, security for 802.11 networks can be simplified into two main components: authentication and encryption. The implementation of these components has been proven insecure and has been extensively documented by the security community.

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and other organizations introduced an end-to-end framework using 802.1X and the EAP to provide this enhanced functionality. Central to this proposal are two main elements:

- EAP allows wireless client adapters, which may support different authentication types, to communicate with different back-end servers such as Remote Access Dial-In User Service (RADIUS)
- IEEE 802.1X, a standard for port-based network access control

To support all popular operating systems, Cisco employees designed and implemented Lightweight Extensible Authentication Protocol (LEAP)—a network-EAP protocol based on 802.1x authentication framework—on Cisco Aironet® WLAN products and solutions. Microsoft's latest operating system, Windows XP, provides support for 802.1x (specifically EAP-TLS and EAP Message Digest 5 [MD5]). Thus, a variety of EAP authentication protocols can be used to authenticate users in today's WLAN networks. Figure 2-1 illustrates the mixed EAP protocol deployment in a WLAN network:

Figure 2-1

Mixed 802.1x Protocol Deployment in a Wireless LAN Network
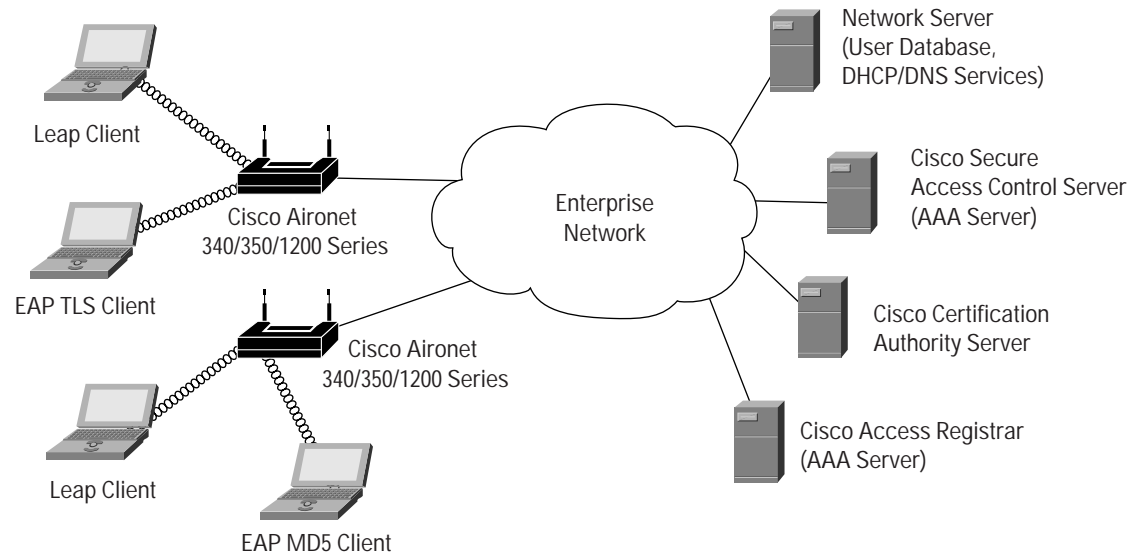
As shown in Figure 2-1, either the Cisco Access Control Server (ACS) or the Cisco Access Registrar can be used for a combined LEAP and EAP-TLS protocol deployment in an enterprise network. Table 2-1 compares the characteristics of the widely available EAP protocols:

Table 2-1 Comparison of Widely Available 802.1x/EAP Authentication Protocols

	802.1x/EAP Compliance	Mutual Authentication	Dynamic Wired Equivalent Privacy Support	Operating System Support
Cisco EAP (LEAP)	Yes	Yes	Yes	Windows platforms (Windows XP, 2000, 98, 95, ME and NT), Windows CE, Linux, Disk Operation System (DOS), and Mac OS
EAP-TLS	Yes	Yes	Yes	Windows XP[1]
EAP MD5	Yes	No	No	Windows XP[1]

1. Note: Microsoft has announced EAP support for legacy operating systems in 2002 (Windows 2000, Windows NT 4, Windows 98, Windows 98 Second Edition, and Windows ME). Also, there are third-party EAP supplicants that provide support for EAP-TLS on various operating systems (Meetinghouse Data Communications EAP supplicant, for example).

As shown in Table 2-1, EAP MD5 does not support mutual authentication nor dynamic derivation of the Wired Equivalent Privacy (WEP) key, which are essential for WLAN networks. Therefore, Cisco recommends that you do not deploy EAP MD5 in a WLAN environment.

This document focuses on EAP-TLS authentication protocol rollout in WLAN networks. Section 3 further introduces the reader to the EAP/802.1x architecture. Section 4 discusses Public Key Infrastructure (PKI) and EAP-TLS authentication protocol. In Section 5, EAP-TLS deployment criteria are examined in detail. Section 6 provides details about the Validation Lab that was built to illustrate an example EAP-TLS rollout in a WLAN network. Section 7 provides EAP-TLS troubleshooting tips. Appendix A details the setup for Windows 2000 Server Certificate Services. Appendix B provides instructions for configuring EAP-TLS using demo certificates (for proof of concept testing).

3 EAP Architecture

EAP provides a standard mechanism for supporting various authentication methods over wired and wireless networks. An authentication, authorization, and accounting (AAA) client (also known as a network access server) such as an access point that supports EAP need not have any understanding of the specific EAP type used in the EAP authentication process. The network access server tunnels the authentication messages between the peer (user machine trying to authenticate) and the AAA server (such as the Cisco Secure ACS). The network access server is aware only of when the EAP authentication process starts and when it ends.

There are EAP types, such as LEAP and EAP-TLS, in which the authentication is mutual: server authenticates user, and user authenticates server. Mutual authentication is usually required in a WLAN environment. For a detailed discussion about designing and implementing WLAN security (including 802.1x/EAP architecture), refer to www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm.

3.1 Relevant RFCs and Drafts

Table 3.1 lists other helpful reference documents.

Table 3.1   Relevant RFCs and Drafts

Document	Title
RFC 2865	Remote Authentication Dial-In User Service (RADIUS)
RFC 2869	Radius Extensions
RFC 2284	Point-to-Point Protocol (PPP) EAP
RFC 2716	PPP EAP-TLS Authentication Protocol
RFC 2246	TLS Protocol

EAP-TLS uses concepts of PKI:

- A WLAN client (that is, a user's machine) requires a valid certificate to authenticate to the WLAN network
- The AAA server requires a "server" certificate to validate its identity to the clients
- The certificate-authority-server infrastructure issues certificates to the AAA server(s) and the clients

Sections 4 and 5 of this document discuss PKI and EAP-TLS authentication protocol in detail.

4 Introduction to PKI and EAP-TLS

EAP-TLS (RFC 2716) is using the TLS protocol (RFC 2246), which is the Internet Engineering Task Force's (IETF's) latest version of the Secure Socket Layer (SSL) protocol. TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

EAP-TLS uses concepts of PKI. The following section introduces PKI and the concepts of certificates, certificate authorization, and validating user identity. A simple example of SSL usage that is familiar to most people will be examined briefly.

4.1 Overview of PKI

A Public Key Infrastructure (PKI) is a management system designed to administer asymmetrical cryptographic keys and public key certificates. It acts as a trusted component that guarantees the authenticity of the binding between a public key and security information, including identity, involved in securing a transaction with public key cryptography.

PKI protects information in several essential ways, described in Table 4-1.

Table 4-1 PKI Protections

Authenticates identity	Digital certificates issued as part of your PKI allow individual users, organizations, and Web site operators to confidently validate the identity of each party in an Internet transaction
Verifies integrity	A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.
Ensures privacy	Digital certificates protect information from interception during Internet transmission
Authorizes access	PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet log-in security and reduce the Message Integration Service (MIS) overhead
Authorizes transactions	With PKI solutions, your enterprises can control access privileges for specified online transactions
Supports nonrepudiation	Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a Web site

Note: EAP-TLS uses the first attribute on this list, identity authentication, as we will see in a later example.

A certificate is a cryptographically signed structure, called the digital certificate, that guarantees the association between at least one identifier and a public key. It is valid for a limited period of time (called the validity period), for a specific usage, and under certain conditions and limitations described in a certificate policy. The authority that issues this certificate is called the certification authority.

A PKI should include at least five components, described in Table 4-2.

Table **4-2** PKI Components

Registration authority	A registration authority provides an interface to all the security management activities that require global coordination to provide a comprehensive and consistent view of security configuration. In its key management function, it registers users needing keys and certificates, collects information required to submit a certification or a revocation request, and connects certification authorities.
Certification authority	A certification authority issues and revokes certificates according to a certification policy. In general, a certification authority is a specialized component that works in an offline mode and is operated by a certification-authority operator according to a certification policy.
Certification authority agent	A certification authority agent is the online front end to a certification authority. Public key certification may be an offline process.
End entity	An end entity may be a certificate holder that is issued a certificate and can sign digital documents or a client that validates digital signatures and their certification path from a known public key of a trusted certification authority.
Repository	A repository is where certificates and revocation lists are stored and made available.

Figure 4-1 shows the PKI architectural model and the interactions between all entities.

Figure 4-1

PKI Architectural Model
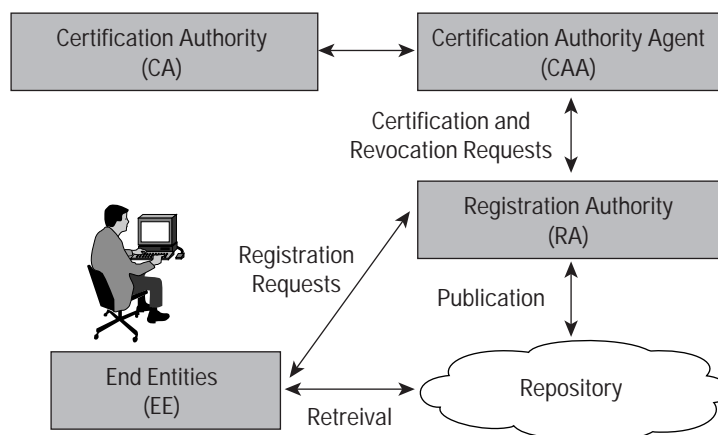
The initialization process consists of setting the necessary configuration for a PKI entity to communicate with other PKI entities. For example, the initialization of an end entity involves providing it with the public key certificate of a trusted certification authority. The initialization of a certification authority involves the generation of its key pair.

During the registration process, an end entity makes itself known to a certification authority through a registration authority before that certification authority issues a certificate. The end entity provides its name and other attributes to be included in its public key certificate(s) and the certification authority (or the registration authority, or both) verifies the correctness of the provided information.

The key pair generation for an end entity may either take place in its own environment or is done by the certification authority (or registration authority). If the key pair is not generated by the end entity itself, then the generated private key must be distributed to the end entity in a secure way (for example, through a secure key distribution protocol, or by using a physical token such as a smart card).

The certification process takes place at the certification authority. After verifying the correctness of the end entity's name and attributes (and that the end entity possess the corresponding private key), the certification authority issues a certificate for the end entity's public key. That certificate is then returned to the end entity or posted in a repository where it is publicly available, or both.

Section 4.1.1 provides an example of PKI usage, and Section 4.1.2 discusses elements of trust in PKI.

4.1.1 The Amazon.com Example

Before sending a credit card number to buy a book at Amazon.com, a customer must verify that the Web site he or she entered is indeed Amazon.com. Also, a secured tunnel between the customer and Amazon must be established to send the credit card number safely. SSL provides this capability. In this case, the customer (using SSL) authenticates Amazon; but note that Amazon does not authenticate the customer. This is called server-side authentication (only the server is authenticated). With EAP-TLS, the RADIUS server authenticates the user, and the user authenticates the RADIUS server. This is called mutual authentication. EAP-TLS authentication will be examined in detail later.

There are two means to verify that Amazon is Amazon. If Amazon and the customer share a secret (a shared secret known only to the customer and to Amazon), the customer is then able to challenge Amazon and to verify that Amazon is holding the shared secret. The problem with this model is that it is impossible for everyone in the world to have a shared secret with everyone else. PKI was invented for this reason. PKI eliminates the need for a shared secret between you and Amazon. Digital certificates are used instead.

4.1.2 Elements of Trust in PKI

PKI authentication requires two elements of trust:

- Private-public key pair
- Certification authority

4.1.2.1 First Element of Trust: Private-Public Key Pair

Every certificate is associated with two keys: a private key and a public key. Only the owner of the certificate knows the private key, whereas the public key (hence its name) is known to everyone. With this key pair, asymmetric encryption is used. A message that was encrypted with the private key can be decrypted only with its corresponding public key and vice versa. Continuing with the example, Amazon encrypts the messages with its private key, and the customer decrypts them using Amazon's public key. In this way, the customer can be sure that any information he or she decrypted with the public key was encrypted using the corresponding private key. In the same way, if one wants to send an encrypted message to Amazon, the message is encrypted using Amazon's public key. Only the holder of

the private key (Amazon.com) is able to decrypt the message. Using this method, a user can validate that Amazon is a legitimate key holder for a given digital certificate. However, trusting that someone is in possession of a digital certificate only provides a name/key-pair binding.

4.1.2.2 Second Element of Trust: Certification Authority

The second element of trust in PKI is the involvement of the certification authority server. Continuing our Amazon.com example, the customer also needs to verify that Amazon is really the entity he or she is communicating with. A third party is needed to validate the identity of Amazon. For this we have the signature of the authority (the certification-authority entity) that issued the certificate to Amazon.

If the customer trusts the certification authority that issued the certificate to Amazon, the user is able to check Amazon's certificate and validate that it is Amazon. The Web browser is configured with a list of trusted root certification authorities. This list is known as a certificate trust list (CTL). Any certificate in this list (that is, the certificate of a root certification authority) is automatically trusted by the client. Also note that a certificate of a trusted root certification authority is self-signed. This is like a passport seal on your passport. You trust the passport because you trust the preparation and identity checking that the passport office made when creating that passport. You trust digital certificates by installing the root certification authority signature for the same reasons.

The certificate is validated using the public-private key pairs of the certification authority. If you trust the certification authority, then you trust this certification authority's certificate. The certification authority's certificate includes the certification authority's public key. In the certificate issued by the certification authority to Amazon, a portion of the certificate is encrypted using the certification authority's private key. When the user receives Amazon's certificate (in the SSL handshake), the Web browser decrypts the encrypted part of the certificate using the certification authority's public key. For example, the certification authority might encrypt this message: "This certificate was issued to Amazon.com. It is valid from 1/1/1995 to 31/12/2015. The URL used by Amazon.com is 'www.amazon.com'..." The encrypted portion of the message contains information about the certificate such as the name of the holder of the certificate, the period for which the certificate is valid, the URL of the holder of the certificate, and so on. Upon completion of the SSL handshake, a user knows he or she is communicating with Amazon.

A new session key is dynamically generated during the SSL handshake. This key is valid for this session only. At the end of SSL handshake, a secured encrypted tunnel is established to Amazon using the session key. (This encryption is symmetric, which is faster and less CPU-intensive than asymmetric encryption.)

4.2 EAP-TLS Model

This section discusses EAP-TLS authentication protocol in detail. EAP-TLS is based on SSL Version 3.0. In EAP-TLS, the SSL handshake is performed over EAP, whereas, on the Internet, the SSL handshake is conducted through Transmission Control Protocol (TCP). Thus, the difference between the SSL handshake in the Amazon example and in EAP-TLS is the transportation layer in which the SSL messages are exchanged.

Note: As with most technologies, EAP has its own terminology for common ideas. In EAP the end user's machine is known as the supplicant, the access point is known as the authenticator, and the RADIUS server is known as the authentication server.

As opposed to the one-way, or server-side, authentication discussed in the Amazon.com example, EAP-TLS performs mutual SSL authentication. This requires both the supplicant (the end user's machine) and the authentication server (the RADIUS server) to have a certificate. In mutual authentication, each side is required to prove its identity to the other using its certificate and its private key. The procedure is the same explained in the Amazon example, but for both sides.

4.2.1 How EAP with TLS Works

As previously mentioned, EAP-TLS authentication is based on 802.1x/EAP architecture. Components involved in the 802.1x/EAP authentication process are: supplicant (the end entity, or end user's machine), the authenticator (the access point), and the authentication server (back-end RADIUS server). The supplicant and the RADIUS server must support EAP-TLS authentication. The access point has to support the 802.1x/EAP authentication process. (The access point is not aware of the EAP authentication protocol type.)

Figure 4-2 illustrates the overall 802.1x/EAP authentication process with EAP-TLS as the authentication protocol. Note that LEAP and EAP MD5 also use the same 802.1x/EAP authentication process.

Figure 4-2
EAP-TLS Authentication Overview
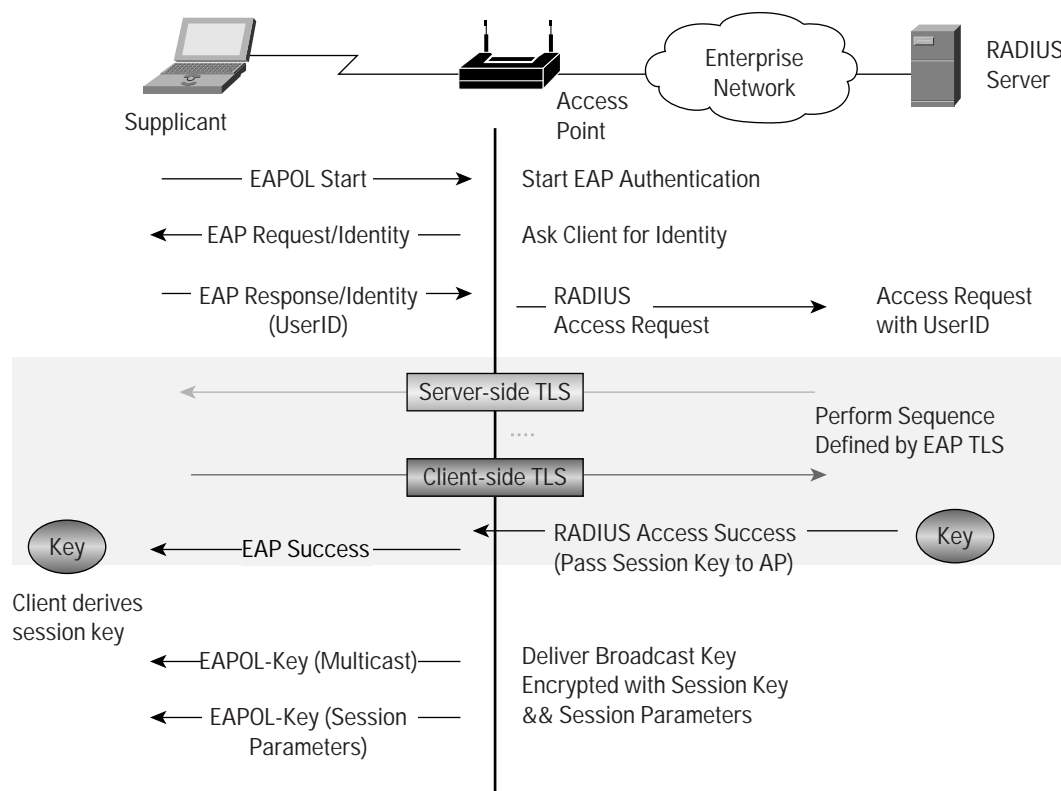
Figure 4-3 illustrates the details of EAP-TLS exchange. The figure shows that, as part of the EAP request, the RADIUS server provides its certificate to the client and requests the client's certificate. The client validates the server certificate and responds with an EAP response message containing its certificate and also starts the negotiation for cryptographic specifications (cipher and compression algorithms). After the client's certificate is validated, the server responds with cryptographic specifications for the session.

Figure 4-3

EAP-TLS Authentication in Detail
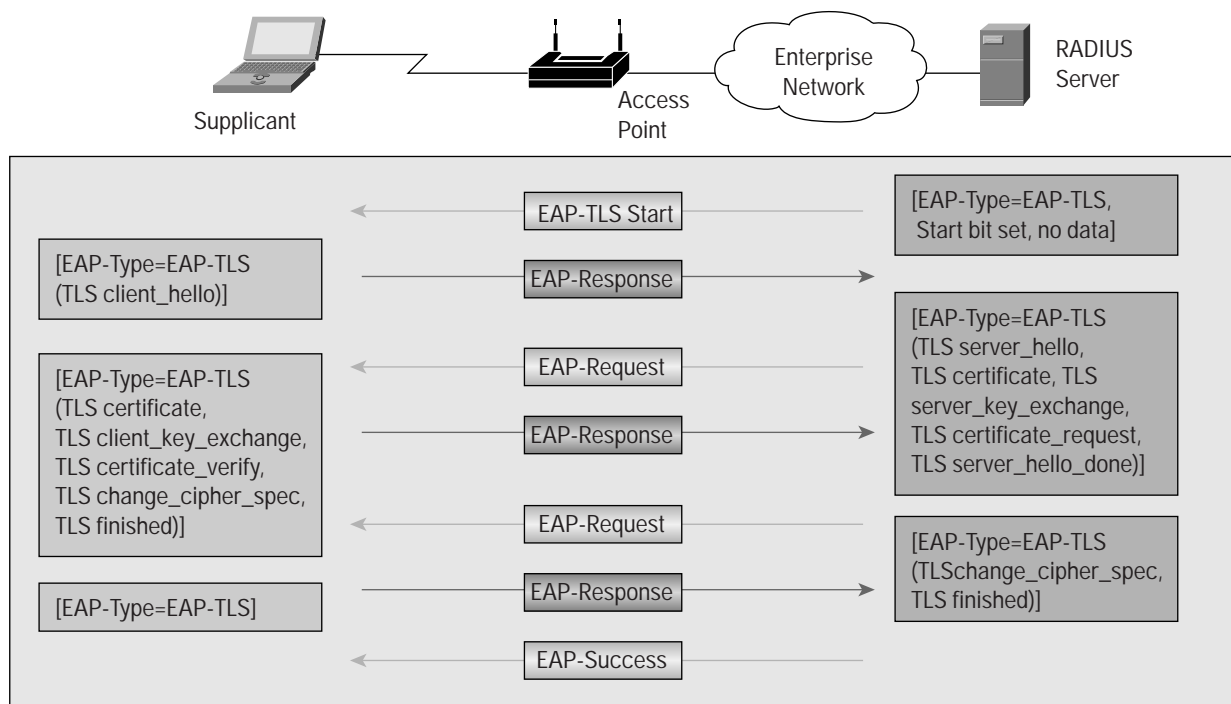
4.2.2 Understanding the Trust Model in EAP-TLS

Before you configure EAP-TLS, you should understand the trust model you are going to implement.

4.2.2.1 Client Trusting Server

This part will help you understand the concept of the client side trust model. Section 6 of this guide provides specific configuration information.

In the client (for example, Microsoft Windows XP), you must configure one root certification authority. Using this root certification authority the client can validate the AAA server (for example, Cisco Secure ACS). For the XP client, no CTL exists. Specify one specific certification authority.

The certification authority you specify to trust can be public or private. If you decide to use a public root certification authority, it is important to understand that you have no control over it. An alternative is to use a private root certification authority for EAP-TLS deployment in your enterprise network. This allows you to build a PKI infrastructure based on a root certification authority sever and possibly several subcertification authority servers (as needed) to issue certificates to both the clients and the AAA servers. (A subcertification authority is a certification authority that is slaved to the root certification authority and unloads some of the burden of certificate processing.)

4.2.2.2 Server Trusting Client

This part will help you understand the concept of AAA server trust model. Specific configuration information is given in Section 6 of this document.

To support EAP-TLS, the AAA server (for example, Cisco Secure ACS) must have a certificate. Either a public certification authority or a private certification authority can be used to issue the AAA server certificate. The AAA server will trust a client certificate that was issued from the same root certification authority that issued its certificate.

If a server certificate was issued from a public certification authority, a client holding a certificate issued from the same root certification authority as the server is allowed in, provided that:

- The name in the certificate corresponds to the username
- The username was found in one of the databases that supports EAP-TLS.

For this reason, and to obtain the highest level of security, it is recommend that the certification authority issuing both clients' and server certificates be a private certification authority.

The AAA server (for example, the Cisco Secure ACS) usually contains a CTL. In the CTL, you can specify as many certification authorities as you intend to trust. Any client holding a certificate issued from a certification authority in the server CTL is allowed in, as long as the name in the certificate corresponds to the username and the username is found in one of the databases that supports EAP-TLS.

Note: In the ACS, by default, the CTL is empty. (In Microsoft Windows, for Web browser usage, the CTL contains the well-known public certification authorities by default.)

4.2.3 Session Key Derivation in EAP-TLS

Figure 4-4 illustrates how the session key is derived at the end of EAP-TLS authentication. As part of the TLS handshake between the server and the client, the client generates a pre-master secret and encrypts it with the server's public key and sends the pre-master secret to the server. Another option would be to use Diffie-Hellman exchange to derive the pre-master secret. The pre-master secret, server and client random values, and "master secret" string value are used to generate a master secret per session. The pseudo-random function (PRF) used to generate the master secret is defined in the TLS RFC (2246). EAP-TLS (RFC 2716) specifies how to derive the session key. The PRF is used again along with master secret, client and server random values, and "client EAP encryption" string value to generate the session keys, Message Authentication Code (MAC) keys and initialization values (for block ciphers only). Note that both the client and the RADIUS server independently derive the session keys. However, the length of the session key is determined by the authenticator (the access point) and is sent in the EAP-over-LAN key message at the end of the EAP authentication to the client (Figure 4-2).

Figure 4-4

Session Key Derivation in EAP-TLS Authentication

```
┌──────────────────┐    ┌──────────────────┐    ┌──────────────────┐
│  Client Random   │    │ Pre-Master Secret│    │  Server Random   │
│ (per connection) │    │   (per session)  │    │ (per connection) │
└──────────────────┘    └──────────────────┘    └──────────────────┘
          \                      │                      /
           \                     ▼                     /
            \              ┌───────────┐              /
             ────────────▶│    PRF    │◀────────────
                           └───────────┘
                                 │
                                 ▼
                        ┌──────────────────┐
                        │   Master Secret  │
                        │   (per session)  │
                        └──────────────────┘
          \                      │                      /
           ────────────▶  ┌───────────┐  ◀────────────
                          │    PRF    │
                          └───────────┘
            ┌─────────────────┼─────────────────┐
            ▼                 ▼                 ▼
┌──────────────────┐ ┌──────────────────┐ ┌──────────────────────┐
│Write MAC Client/ │ │  IV Client/Server│ │ Write Secret Client/ │
│     Server       │ │ (per connection) │ │       Server         │
│ (per connection) │ │                  │ │   (per connection)   │
└──────────────────┘ └──────────────────┘ └──────────────────────┘
```
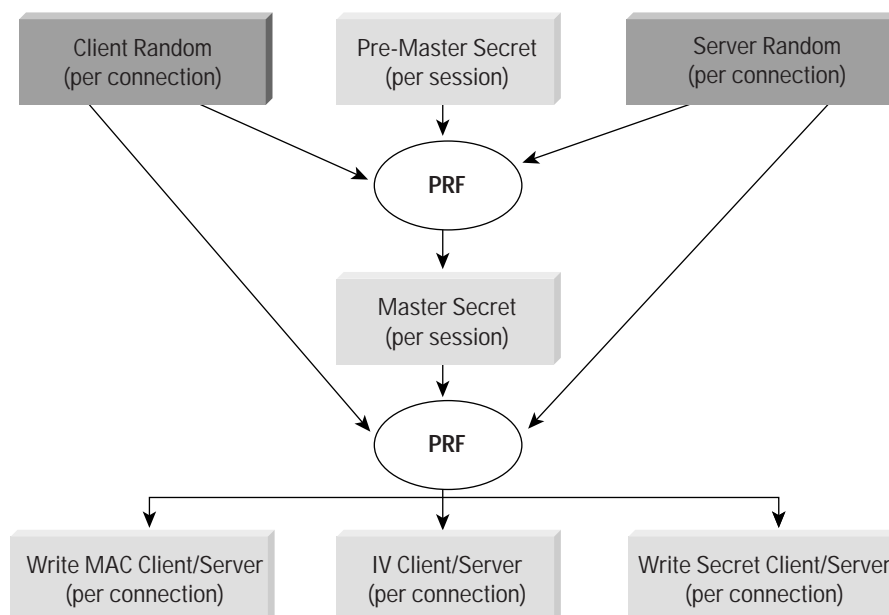
5 EAP-TLS Deployment in a WLAN Environment

This section details the system components that are required to roll out EAP-TLS in an enterprise network. Certificate requirements, both for the AAA server and the clients, are discussed in detail. Deployment issues, such as mixed EAP protocol deployment and AAA server scalability, are addressed in sections 5.3 and 5.4.

5.1 System Components

Table 5.1 lists the components that are required for accessing a wireless LAN network using EAP-TLS authentication:

Table 5-1   Components for Accessing a Wireless LAN Network

Access point(s)	Cisco Wireless Access Point, operating system Version 11.06 or later, or equivalent device
AAA/RADIUS server	Cisco Secure ACS for Windows Version 3.0 or later, Cisco Access Registrar v3.0 or any other AAA/RADIUS server that supports EAP-TLS and supports Enhanced Key Usage (see Figure 5-1)
Client(s) (user machines)	Microsoft XP (other clients for non-XP operating systems may be available)[1]
Certification authority server	Microsoft certification authority server or any other certification authority server that supports Enhanced Key Usage (see Figure 5-1)

1. Note: Microsoft has announced EAP support for legacy operating systems in 2002 (Windows 2000, Windows NT® 4, Windows 98, Windows 98 Second Edition, and Windows ME). Also, there are third-party EAP supplicants that provide support for EAP-TLS on various operating systems (for example, Meetinghouse Data Communications EAP supplicant).

5.2 Certificate Requirements

This section discusses the certificate requirements on both the client and the AAA server sides.

5.2.1 Client Certificate Requirements

For a client (using Windows XP professional, for example) to authenticate using EAP-TLS, the client must obtain a personal client certificate. This certificate must meet several requirements:

Figure 5-1
Client Certificate and the Enhanced Key Usage Field
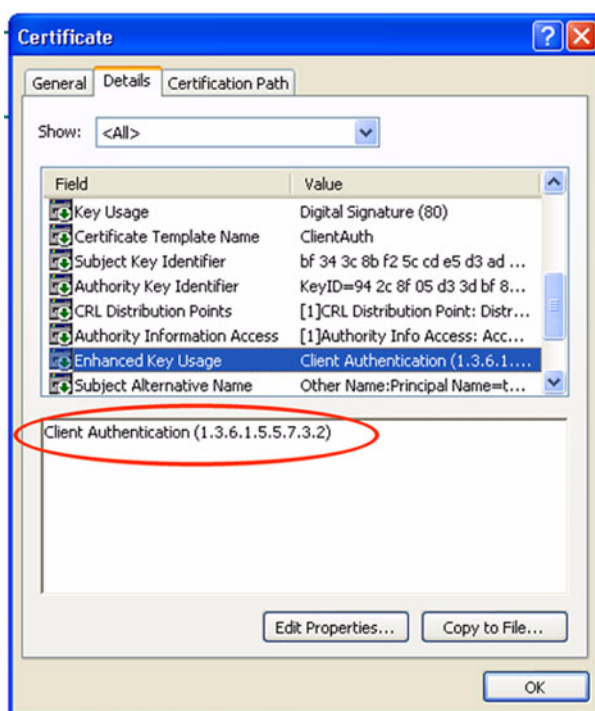
- The certificate has to be installed when the requested user is logged in to the machine. A personal certificate that will be installed when a different user is logged in will not be accessible by the requested user.
- The certificate has to be X.509 Version 3 (as shown in Figure 5-1).
- The certificate must have the Enhanced Key Usage (EKU) field. For the client certificate, the EKU field must contain the Client Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.2" as shown in Figure 5-1).
- The subject name in the certificate must correspond to the user account name (either a username or the user ID of the account). This account name has to exist in one of the databases that support EAP-TLS. If, for example, the user account name is "TME USER5" (first name=TME, last name= USER5), the cn part of subject name in the certificate has to be "TME USER5" (as shown in Figure 5-2). Alternatively, as an example, if the account name is "eaptls1" (user ID is used instead of the username), the cn part of the subject name in the certificate has to be "eaptls1" (as shown in Figure 5-3). The @domainName.xxx part, if it exists, is not used in comparison.

Figure 5-2
Client Certificate: Subject/cn Field
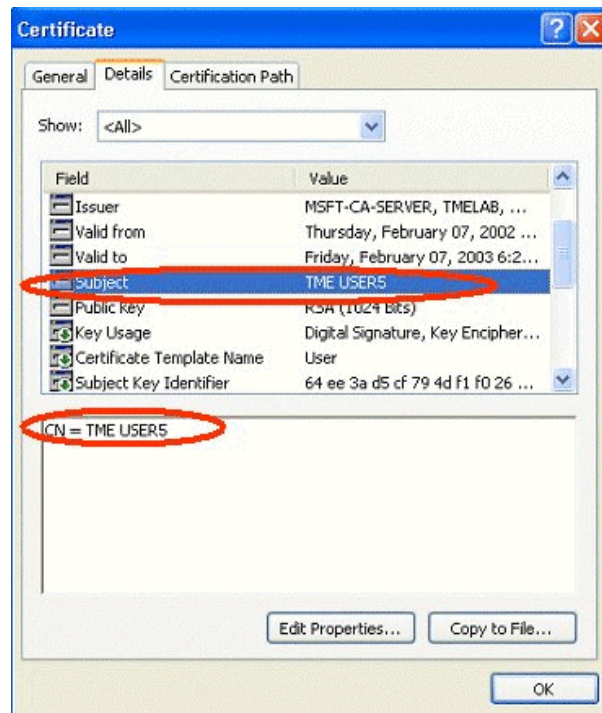
Figure 5-3
Client Certificate 2: Subject/cn Field
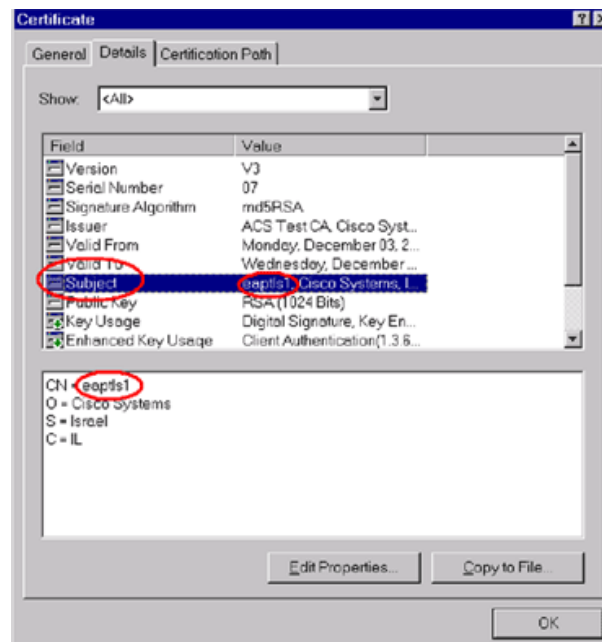
- The client must have the corresponding private key. To verify that the private key exists, view the general section of the certificate and verify that you see the following message: "You have a private key that corresponds to this certificate" (Figure 5-4).
- When viewing the certificate, you have to verify that the following statement appears: "This certificate is intended to: Guarantee your identity to a remote computer" (Figure 5-4).
- When viewing the certificate you have to verify that the certificate date is valid. You can view the certificate "Valid from 12/3/2001 to 12/3/2003" (Figure 5-4).

Figure 5-4
Client Certificate: Date and Private Key Verification
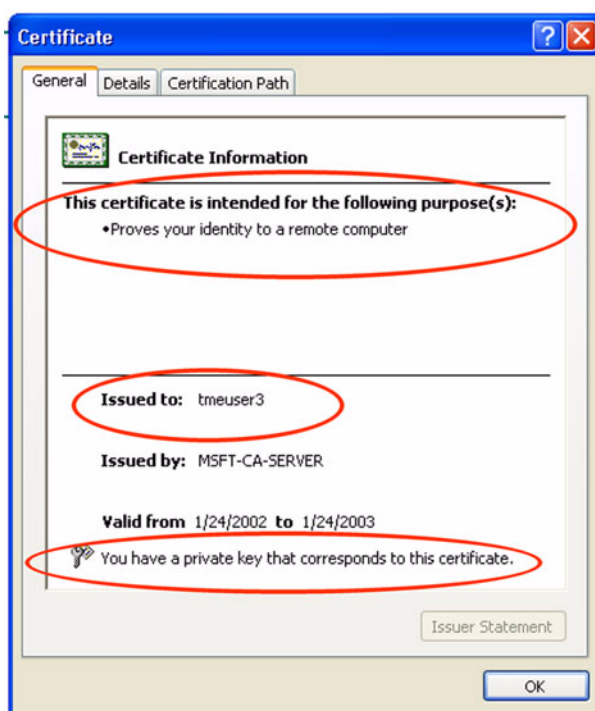
5.2.2 AAA Server Certificate Requirements

For the server certificate installed on the AAA server several requirements must be met. (You should also read AAA server documentation before configuring the certificate.)

- The certificate must be X.509 Version 3 (Figure 5-5).
- The certificate must have the EKU field. For the server certificate, the Enhanced Key Usage must contain the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1") (Figure 5-5).
- The AAA server must have the private key in order to use the certificate.

Figure 5-5

Server Authentication Certificate
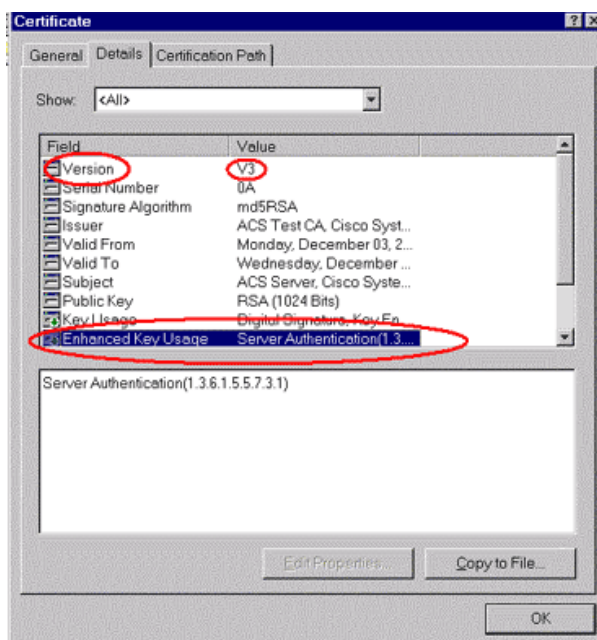
5.3 Mixed EAP Protocol Deployments

The Cisco Aironet access point passes through any EAP authentication type presented to it by a client. It is up to the authentication server (RADIUS server) to accept or reject the authentication type and respond accordingly. In the situation of EAP-TLS, the AAA/RADIUS server must be able to reject the presented authentication type and respond with the desired type.

For example, Cisco Secure ACS supports fallback from LEAP to EAP-TLS. By default, ACS initially employs LEAP authentication when a client initiates EAP authentication (only if the access point is configured for Cisco Aironet as the RADIUS network-access-server type). If the client is a LEAP client, LEAP is used. If it is not a LEAP client, the client sends an EAP negative-acknowledgment (NAK) message with the desired EAP type. If this type is EAP-TLS and the ACS is configured to do EAP-TLS, the ACS starts EAP-TLS.

5.4 AAA Server Scalability

The AAA server's scalability plays a role in EAP-TLS deployment. The number of EAP-TLS clients along with EAP-TLS authentications per second (both worst case and average scenarios) must be considered when assessing the appropriate scalability and availability for the AAA servers.

As an example, though formal testing on ACS using EAP-TLS has not been performed, informal testing indicates a performance reduction, when compared with LEAP, because of the increased computation requirements of PKI over LEAP. A 20-30 percent reduction can be expected. With this in mind, LEAP has tested to perform 40-60 authentications per second. With the maximum expected performance reduction, you can reasonably expend .7 x 60, or 42, authentications per second using EAP-TLS.

You can calculate the load on ACS by applying this formula: (session length)/(number of connections). Using a value of 25 connections per access point and a 10-minute (600-second) session timeout to force WEP rekeying, you get 600/25 = 24 seconds/connection, which translates into 1 transaction every 24 seconds, or 1/24 (0.042) transactions per second. Table 5-1 below shows the transaction requirements for ACS based on the number of fully loaded access points being supported by a single ACS system.

Table 5-2 RADIUS Server Loading

Number of Access Points	Number of Connections	Session Duration (Minutes)	Session Duration (Seconds)	Session Duration Per Connection	Transactions Per Second (TPS)
1	25	10	600	24	0.042
1	25	30	1800	72	0.014
1	25	60	3600	144	0.007
10	250	10	600	2.4	0.417
10	250	30	1800	7.2	0.139
10	250	60	3600	14.4	0.069
100	2500	10	600	0.24	4.167
100	2500	30	1800	0.72	1.389
100	2500	60	3600	1.44	0.694
1000	25000	10	600	0.024	41.667
1000	25000	30	1800	0.072	13.889
1000	25000	60	3600	0.144	6.944

From this table we can see that a single ACS could support about 1,000 access points with a rekey time of 10 minutes. As the rekey time is extended, the number of access points that a ACS can support increases. Conversely, any decrease in rekey time or increase in number of users per AP results in an increase of TPS and a lowering in the number of access points that a ACS can support.

Note that this does not take into account issues of network latency and loading, delays caused by external database usage, or network topographical issues.

Note: You can use Table 5-2 to determine the scalability of other RADIUS servers using EAP-TLS if you know the maximum number of transactions per second the RADIUS server can support when running EAP-TLS.

From a practical standpoint, the RADIUS server should be inside the general network, preferably within a secure subnet designated for servers, such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and so on. You should avoid requiring RADIUS requests to travel over WAN connections because of possible network delays and loss of connectivity. This is not always possible because of various reasons (that is, small, remote subnets requiring authentication support from the enterprise intranet). These issues are illustrated in Figure 5-6.

Figure 5-6
Network Topology
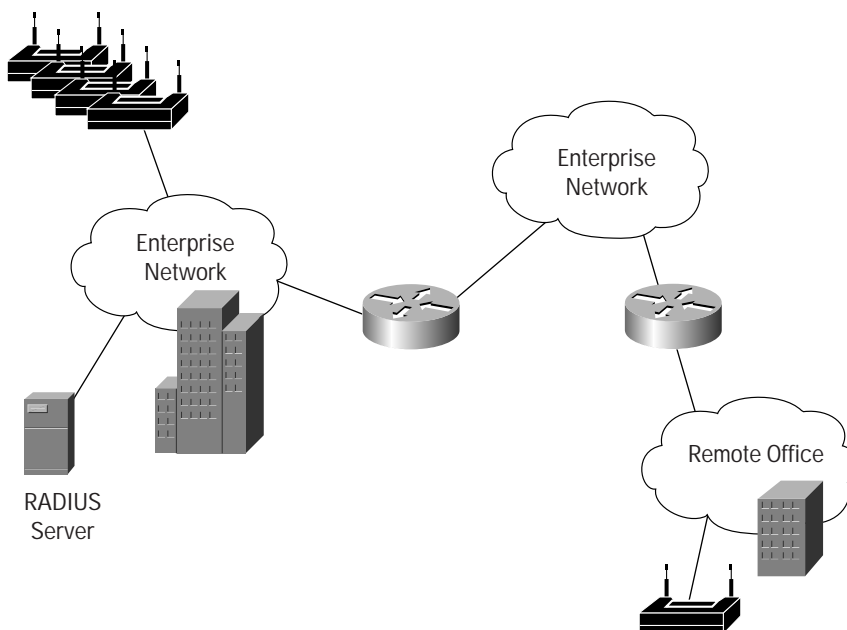
You must also consider backup authentication. You may use a system that is dedicated as the RADIUS secondary. Or you may have two synchronized systems that each support a different network segment but provide mutual backup if one fails. Refer to the documentation for the RADIUS server in use for database replication and the use of external databases.

6 Validation Lab

The authors built a Validation Lab to configure and test EAP-TLS deployment in an enterprise network scenario. Figure 6-1 illustrates the Validation Lab setup:

Figure 6-1
Validation Lab
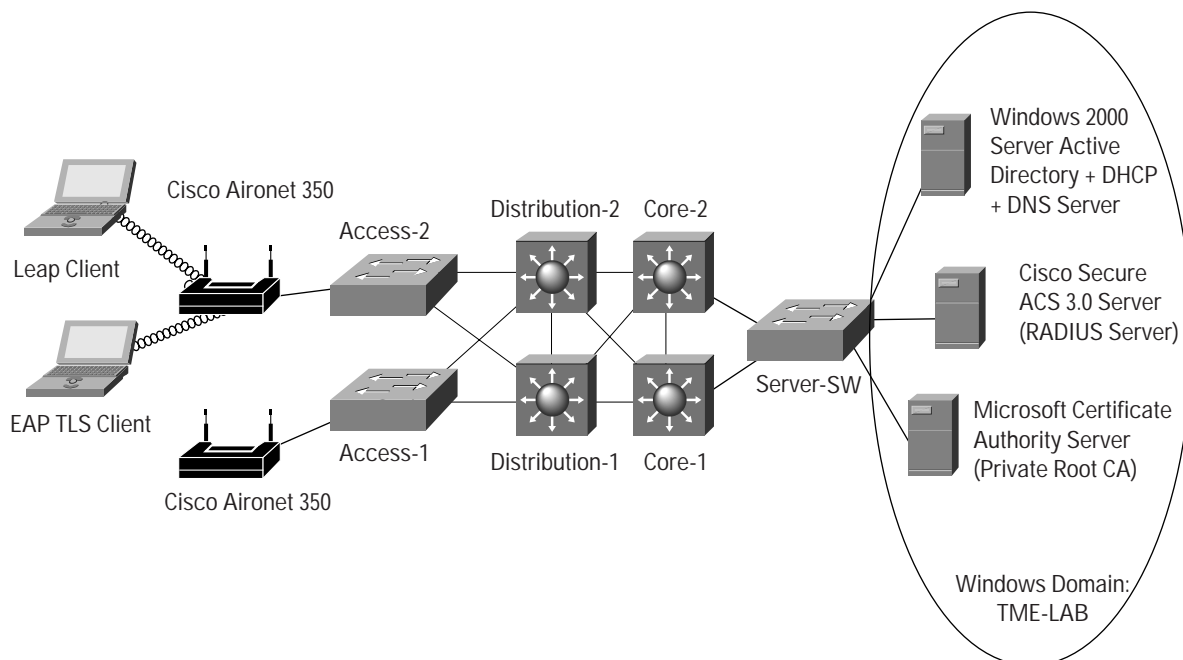
The following sections discuss the Validation Lab setup and configuration in detail. Configuration information is provided for the Cisco Aironet access point, Cisco Secure ACS v3.0, and the Microsoft Windows XP Client. Note that several different RADIUS servers and certification authority servers could be used for EAP-TLS deployment, as noted in Section 5.1.

6.1 System Components

Following are descriptions and prerequisites for the Validation Lab components:

- Cisco Aironet access point—Minimum access point firmware of 11.06 for 802.1x Draft 10, recommended 11.10T or the latest version.
- Cisco Secure ACS v3.0—Cisco Secure ACS provides the AAA server functionality in a wireless/wired LAN network; Version 3.0 provides support for LEAP, EAP-TLS, and EAP MD5 authentication (802.1x) protocols.
- Microsoft XP Professional Client—Provides support for standards-based 802.1x authentication protocols such as EAP-TLS and EAP MD5.
- Microsoft 2000 Client—An Example LEAP client in an enterprise WLAN network.
- Microsoft certification authority server—Microsoft Windows 2000 Server running Microsoft Certification Authority Services; this is a private root certification authority server. Using a private root certification authority is preferred for enterprise PKI certificate distribution and management.
- Microsoft 2000 Server—Providing Active Directory Services for user management, DHCP, and DNS services (if preferred, DHCP and DNS services could run on individual servers).

6.2 ACS Configuration

This section discusses the steps required to configure the ACS v3.0 for EAP-TLS. (For information about generic ACS configuration details, refer also to ACS documentation.)

Configuring ACS for EAP-TLS requires three stages:

- Obtaining a ACS certificate
- Configuring ACS "System Configuration" parameters to enable EAP-TLS
- Configuring the appropriate network-access-server type for the access point in Network Configuration

6.2.1 Obtaining the Server-Side Certificate

As discussed in Section 4, the ACS server must obtain a server certificate from the enterprise root certification authority server to authenticate a WLAN EAP-TLS client. Obtaining a server certificate and installing it onto the ACS may be accomplished in one of these ways:

- Obtain a certificate file and private key file in any way you like and install it on the ACS (certificate file has to be base-64 encoded)
- Have a certificate in storage (local machine store) including private key and specify the name

In the Validation Lab, the second method was used. A Web browser on the ACS was used to obtain a server certificate from the private Microsoft root certification authority server. The obtained server certificate was installed onto the local machine store of the ACS.

Refer to Appendix A for instructions on how to configure the Microsoft certification authority server. Following is the procedure used to obtain a server certificate from a Microsoft certification authority server:

1. On the local ACS machine, point the browser at the Microsoft certification authority server as follows: http://IP-address-of-Root-CA/certsrv.

2. Log in as the Administrator.

3. Choose "Request a certificate" and click Next.

4. Choose "Advanced request" and click Next.

5. Choose "Submit a certificate request to this CA using form" and click Next.

6. Choose/specify the following options on the Advanced certificate request form:

   a. Choose "Web Server" as the certificate template.

   b. Specify the name for the certificate being issued to the ACS.

   c. Specify 1024 bits as the key size.

   d. Choose "Mark keys as exportable."

   e. Choose "Use local machine store" and click Next.

7. Web browser should pop up with a message "Certificate Issued." Click "Install this certificate." This should result in successful installation of a server-side certificate (for EAP-TLS authentication) on the ACS.

Figure 6-2 illustrates steps 2 and 3 (from the above procedure) for obtaining a server certificate from a Microsoft certification authority server.

Figure 6-2

Steps 2 and 3 for Server Certificate Installation
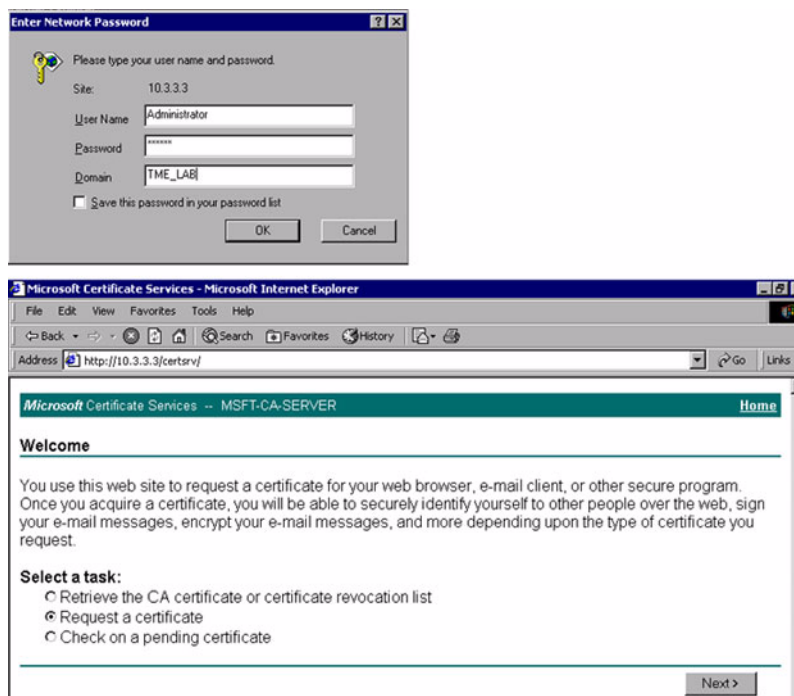
Figure 6-3 illustrates steps 3 and 4 for obtaining the server certificate from a Microsoft certification authority server. As shown in the figure, an advanced request form is used to submit a certificate request to the certification authority server.

Figure 6-3
Steps 3 and 4 for Server Certificate Installation

Figure 6-4 illustrates the configuration required on the advanced certificate request form to obtain the server certificate. It is important to note the name given to the certificate; the name has to be specified when enabling EAP-TLS authentication on the ACS.

Figure 6-4
Step 5 for Server Certificate Installation

Figure 6-5 shows the steps required to install the server certificate onto the ACS local machine store.

Figure 6-5
Steps 6 and 7 for Server Certificate Installation

After you have completed these steps, a server certificate will be installed on the ACS's local machine store.

Server certificate verification:

The server certificate obtained should match the criteria specified in Section 5. Use the following procedure to verify the certificate issued to the ACS server:

1. On the Microsoft certification authority server, find the ACS server certificate under "Issued Certificates."

2. Double-click the ACS server certificate and ensure that all criteria specified in Section 5 are met.

6.2.2 System Configuration Parameters on ACS

After obtaining the ACS server certificate from the enterprise root certification authority server, the following steps were used to configure the ACS for EAP-TLS (and LEAP) authentication:

1. On the ACS menu, choose System Configuration >> ACS Certificate Setup.

2. Under ACS Certificate Setup, choose "Use existing certificate" and then the "Specify certificate from storage" option. Specify the name of the ACS certificate obtained from the certification authority server (in our example, "ACS-TMELAB" was specified in Section 6.2.1). Click Submit.

3. On the ACS menu, choose System Configuration >> "Certification Authority Setup." Click "Edit certificate trust list" and select the name(s) of the certification authority server(s) that were used to issue certificates to the ACS device(s) and EAP-TLS clients.

Note: The certificate trust list (CTL) has to be used when the root certification authority (ex: Root_CA_A) that issued the ACS certificate and the root certification authority that issued the client(s) certificate (Root_CA_B) are not the same. In this scenario, Root_CA_B has to be added to the ACS trust list. To do this, add the certificate of Root_CA_B to the ACS CTL. By default, ACS trusts certificates that were issued from the same root certification authority that issues its certificate. In our example (in the Validation Lab), we used the same root certification authority to obtain the ACS and client certificates; thus, the ACS will automatically trust the client certificates and you do not need to edit the CTL.

4. Choose the ACS menu and choose System Configuration >> Global Authentication Setup. Select the "Allow EAP-TLS ..." option and click the "Submit+Restart" button.

The following figures illustrate the above steps needed to configure the ACS for EAP-TLS:

Figure 6-6 shows the System Configuration menu options for EAP-TLS setup on the ACS.

Figure 6-6
ACS System Configuration Parameters
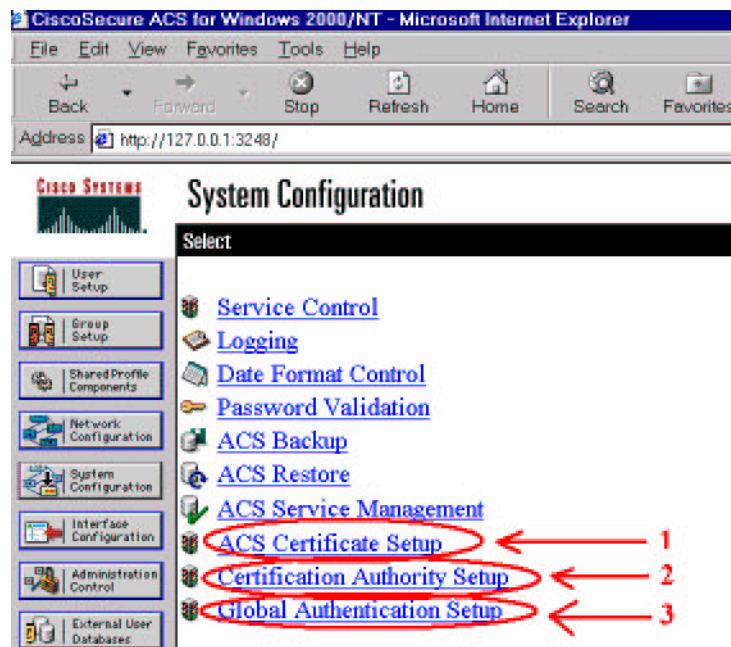
Figure 6-7 shows the required configuration for server certificate setup. As shown in the figure, the name of the certificate that was installed on the ACS local machine store (as discussed in Section 6.2.1) is specified under the option "Use certificate from storage."

Figure 6-7
Cisco Secure ACS System Configuration: ACS Certificate Setup Options
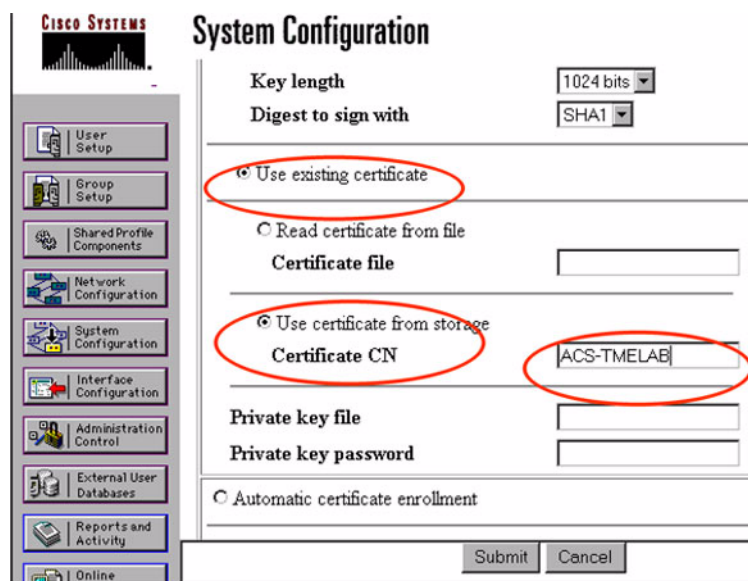
Figure 6-8 shows the global authentication setup under system administration. After enabling EAP-TLS authentication, click the "Submit+Restart" button for the changes to take effect.

Figure 6-8
Cisco Secure ACS Server System Configuration: Global Authentication Setup

6.2.3 Cisco Secure ACS Network-Access-Server Type Configuration

When adding the Cisco Aironet access point as a network access server to the ACS, several "Authenticate Using" options (that is, network-access-server types) are available. Choose "RADIUS (Cisco Aironet)" if the enterprise WLAN will have a mixed deployment of LEAP and EAP-TLS clients. However, if only EAP-TLS/EAP MD5 authentication is preferred, then choose "RADIUS (IETF)" option.

Figure 6-9 shows the access point configured to allow a mixed deployment of EAP-TLS and LEAP clients.

Figure 6-9

ACS >> Network Configuration >> AP>> "NAS type"
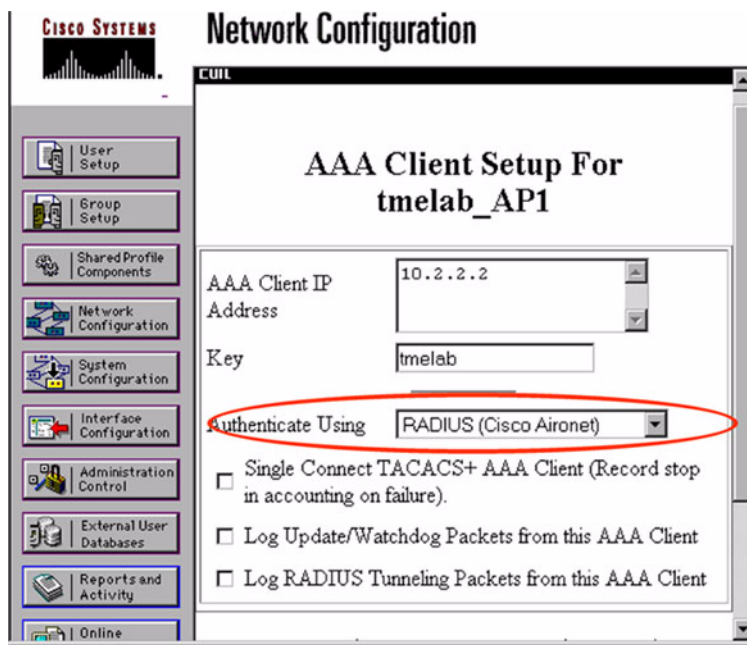
6.3 Cisco Aironet Access Point Configuration

As stated in sections 3 and 4, the access point can be configured to be a network access server for the 802.1x authentication process. The access point is capable of "understanding" and translating from 802.1x to RADIUS protocol (to communicate with the AAA server). However, the access point is not "aware" of the type of 802.1x authentication process taking place (that is, it does not know whether it is LEAP, EAP-TLS, or EAP MD5). This section details the required configuration on the access point to support the 802.1x authentication process.

The following procedure was used to configure the access points for 802.1x authentication in the Validation Lab:

1. Using the Web browser (as shown in Figure 6-10), verify that the access point version is 11.06 or later.

Figure 6-10

Cisco Aironet AP Firmware Version
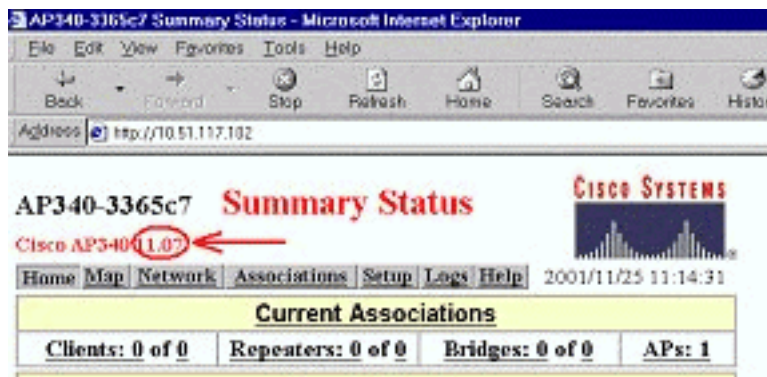
2. Click Setup and then Security. On the Security Setup page, click Authentication Server link (as shown in Figure 6-11).

Figure 6-11
Security Setup Page
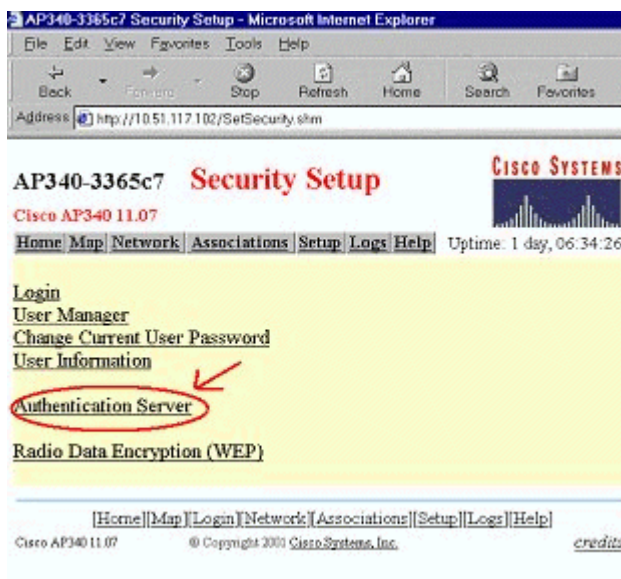
3. On the "Authentication Configuration" page (see Figure 6-12):

    a. Choose "DRAFT 10" for 802.1x Protocol Version.

    b. Configure the AAA server (ACS server) information as follows:

        i. Enter the ACS IP address.

        ii. Enter 1645 or 1812 (default) for port number.

        iii. Enter the shared secret between the ACS and the access point (also configured in ACS).

        iv. In "Use Server for," check EAP Authentication.

Figure 6-12

Authentication Configuration Page on the Cisco Aironet AP

4. Go back to the Security Setup page and click "Radio Data Encryption (WEP)" link (as shown in Figure 6-13).

Figure 6-13

Security Setup Page on the Cisco Aironet AP

5. On the AP Radio Data Encryption page (see Figure 6-14):

a. Choose "Full Encryption" as Use of Data encryption by Station.

b. For enabling EAP-TLS authentication (also enables EAP MD5):

    i. Check Open in "Accept Authentication Type."

    ii. Check "Require EAP" (only under open authentication).

c. For enabling LEAP authentication, select the "Network-EAP" option.

d. Set WEP Key 1 for Broadcast Key (in 11.10T and later releases, you can also enable broadcast key rotation).

e. Click Apply.

Figure 6-14
AP Radio Data Encryption Page

After the preceding steps have been completed, the access point is configured to allow only LEAP and EAP-TLS/MD5 clients to authenticate to the enterprise wireless LAN network.

6.4 Microsoft XP Client Configuration

The following procedure was used to configure a Windows XP client to authenticate to a WLAN network using EAP-TLS:

1. Obtain and install a client certificate; refer to Section 6.4.1.

2. Configure networking parameters on Microsoft XP Networking; refer to Section 6.4.2.

6.4.1 Obtaining the Client-Side Certificate

As discussed in Section 4, the client must obtain a certificate from a certification authority server for the ACS to authenticate a WLAN EAP-TLS client. Several ways of obtaining a client certificate and installing it onto the Windows XP machine are available. To acquire a valid certificate, the Windows XP user has to be logged in using his or her user ID and has to have a network connection (either a wired connection or a WLAN connection with 802.1x security disabled).

In the Validation Lab, a Web browser on the Windows XP client and a wired connection to the network were used to obtain a client certificate from the private root certification authority server. The following procedure was used to obtain the client certificate from a Microsoft certification authority server:

1. Using a Web browser on the client, point the browser to the certification authority server as follows: http://IP-address-of-Root-CA/certsrv.

2. Log in using "Domain_Name\user_name"; you must log in using the username of the individual who will be using the XP client. (The username gets embedded into the client certificate.)

3. On the "Welcome" screen, choose "Request a certificate" and click Next.

4. Choose "Advanced request" and click Next.

5. Choose "Submit a certificate request to this CA using a form" and click Next.

6. On the advanced certificate request form, choose the following (as shown in Figure 6-15):

   a. Certificate Template as "Authenticated Session."

   b. Specify Key Size to be 1024. Click Submit.

7. On the "Certificate Issued" screen, click "Install this certificate"; this should result in successful installation of a client certificate on the Windows XP client.

Figure 6-15

Step 6: Advanced Certificate Request for Obtaining a Client Certificate

Client certificate verification:

The client certificate should conform to the requirements specified in Section 5.2.1. The following procedure was used to verify the client certificate on the Windows XP machine:

1. Using Microsoft Internet Explorer, choose Tools >> Internet Options >> Content >> Certificates; a certificate with the name of the logged-in user ID/username should be present (as shown in Figure 6-16).

Figure 6-16
Microsoft Internet Explorer: Client Certificate Verification
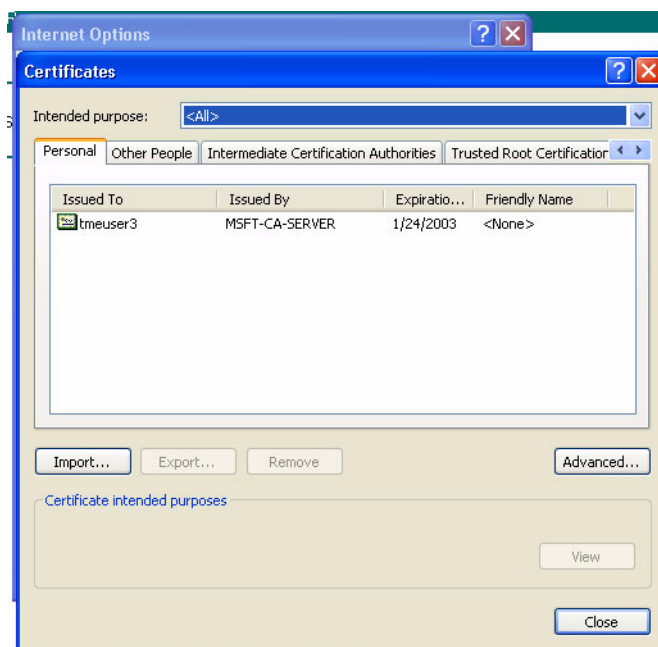
2. Double-click the certificate and verify the following (as stated in Section 5.2.1):

a. Under the "General" section, verify the following (as shown in Figure 6-17): Purpose of the certificate is "Proves your identity to a remote computer." The "Issued to" field should contain the user ID or the username of the XP client, and a message should indicate, "You have a private key that corresponds to this certificate."

b. Under the "Details" section, verify the following (as shown in Figure 6-18): "Subject" field corresponds to the username or the user ID used to generate and install the certificate on the XP machine, and the "Enhanced Key Usage" field (as shown in Figure 6-19) should contain "Client Authentication code (1.3.6.1.5.5.7.3.2)". Refer to Section 5.2.1 for more details about the Enhanced Key Usage field.

c. Under the "Certification Path" section, verify the following statement: "This certificate is OK." Verify that the whole path of certificates until the root (the trusted root certification authority) has been installed (refer to Figure 6-20).

Page 31 of 42

Figure 6-17
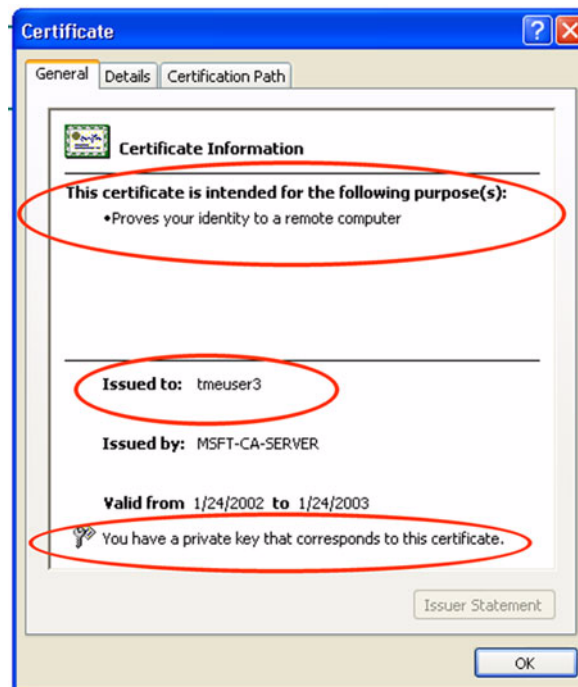Client Certificate Verification: "General" Section

Figure 6-18
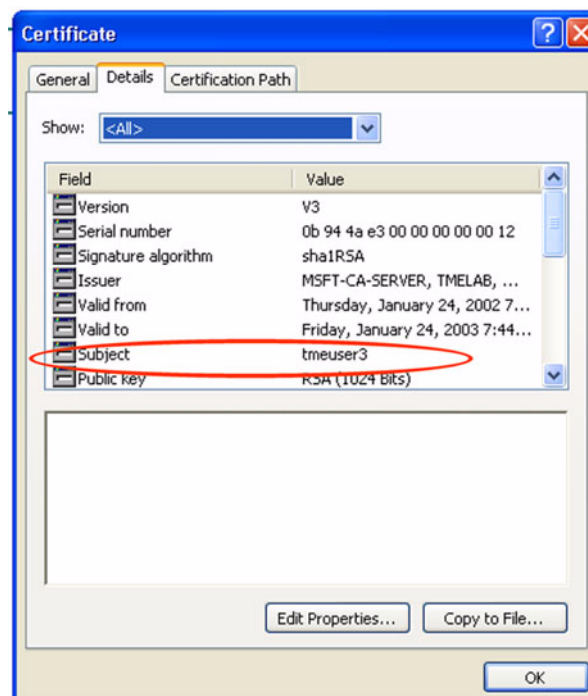Client Certificate Verification: "Details" Section

Figure 6-19

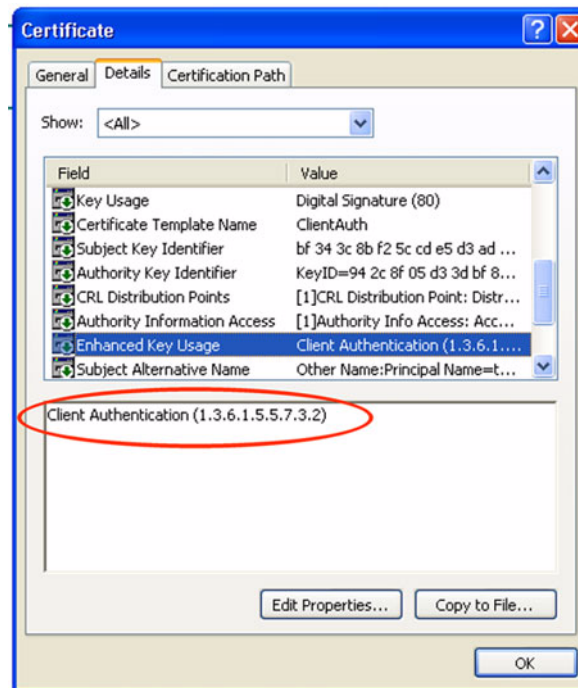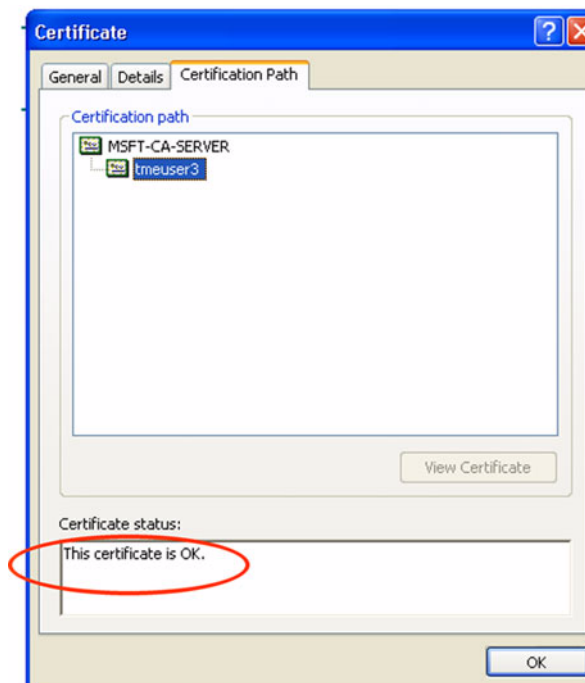Client Certificate Verification: "Details" Section, EKU Field

Figure 6-20

Client Certificate Verification: "Certification Path" Section

6.4.2 Microsoft Windows XP Wireless Networking Configuration

The Microsoft XP client wireless LAN networking should be configured to enable EAP-TLS authentication to the WLAN network. The following procedure was used to configure the XP machine:

1. In Microsoft XP >> Control Panel >> Network Connections configuration: Double-click the Wireless Network connection.

1. In "Authentication" section, configure the following options:

    a. Select "Enable network access control using IEEE 802.1x" (see Figure 6-21).

    b. Select EAP type as "Smart Card or other Certificate"; click Properties:

    i. Select the "Use a certificate on this computer" option.

    ii. Choose the "Validate server certificate" option and click "Trusted root certificate authority" and select the root certification authority server for the enterprise EAP-TLS clients and ACS device(s) (refer to figure 6-22).

    iii. Click "OK."

2. In the "Wireless Networks" section, configure the following options:

    a. Under Preferred networks, select the WLAN network (displayed using the Service Set Identifier [SSID] name of an access point) and click Properties (refer to figures 6-23 and 6-24).

    i. Select the "Data Encryption (WEB enabled)" option.

    ii. Select the "The key is provided for me automatically" option.

    iii. Click "OK."

Figures 6-21 through 6-24 illustrate these three steps:

Figure 6-21
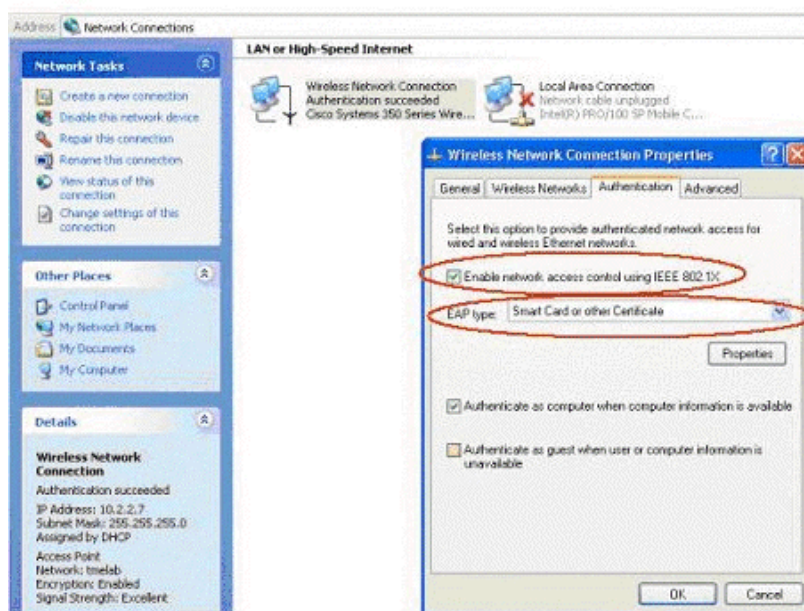MS XP Client >> Network Connections >> Wireless LAN >> Authentication

Figure 6-22

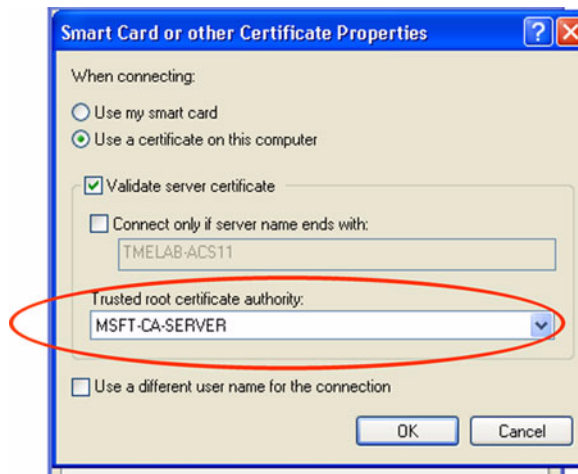EAP-Type (Smart Card or Other Certificate) Properties

Figure 6-23

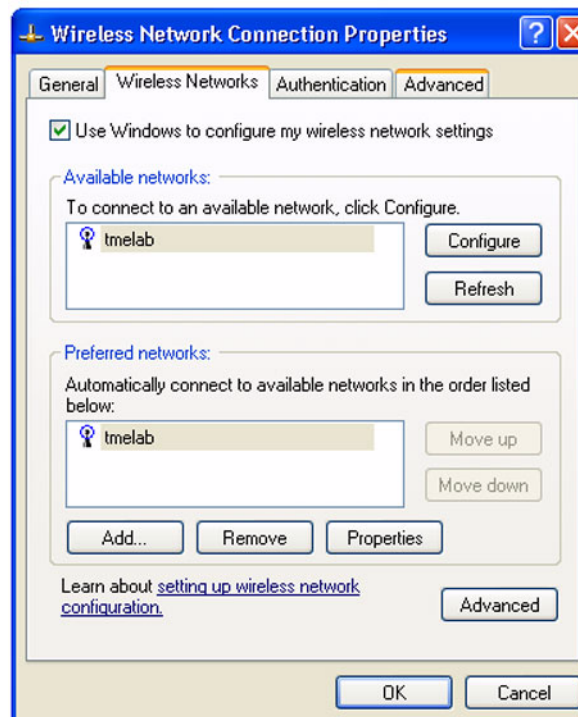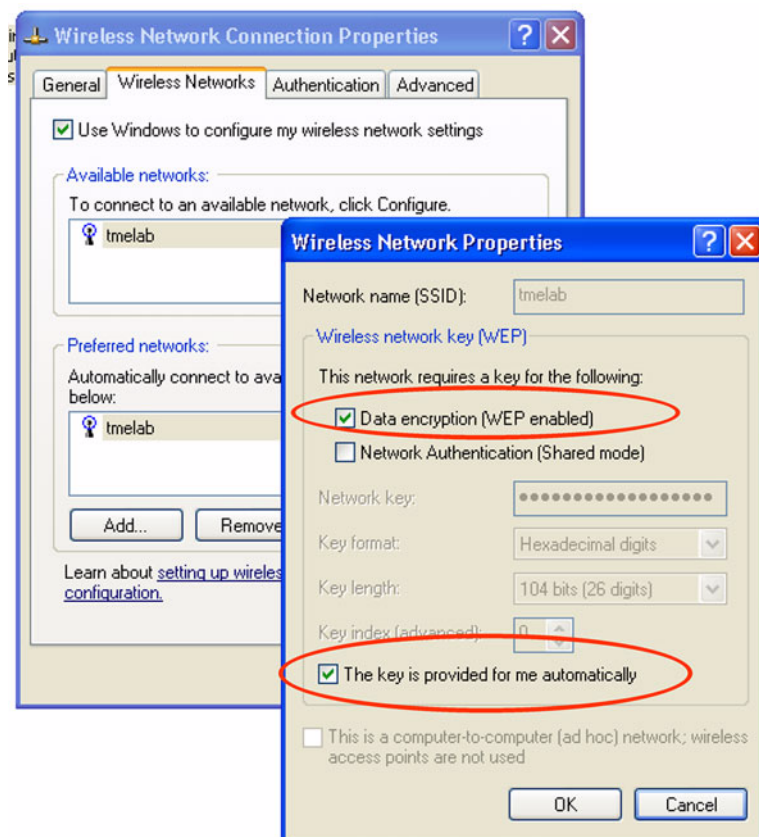Wireless Network Connection Properties

Figure 6-24
Wireless Networks Properties Configuration

At the end of above configuration steps, Microsoft XP clients should be able to authenticate to the enterprise WLAN using EAP-TLS.

6 Troubleshooting Tips for EAP-TLS

A modular troubleshooting approach is recommended for EAP-TLS. As discussed earlier in this document, three major components of EAP-TLS are EAP-TLS client, network access server (the access point), and the AAA server. Certification authority server infrastructure is also covered in this section.

Following are some troubleshooting tips for EAP-TLS:

1. Verify the configuration of the access point as described in Section 6.3.

2. Verify the configuration of Windows XP as described in Section 6.4. Ensure that EAP-TLS is configured for the user account. (Be aware that multiple user accounts and profiles could exist on a Windows XP client.)

3. If you see a message that indicates that Windows XP is failing to find a certificate to authenticate to the network, verify that you have installed a client certificate for the user account. The client certificate is invalid if the EKU field does not contain the "Client Authentication" OID (as described in sections 5.2.1 and 6.4.1).

4. Verify that the client certificate is formatted as X.509 Version 3.

5. Verify that the user account is the same name (username or user ID) as in the certificate.

6. Verify the configuration of the AAA server (ACS configuration is specified in Section 6.2). If the EAP-TLS clients and the AAA server(s) did not use the same root certification authority, then verify that the whole chain of certification authority servers' certificates have been installed on the AAA server. The same applies if the certificate was obtained from a subcertification authority.

7. Verify that the user account exists in the internal database of the AAA server or on one of the configured external databases.

8. Verify that the AAA server certificate contains EKU with the "Server Authentication" OID (as described in Section 5.2.2).

9. Verify that AAA server certificate complies with X.509 Version 3.

Figures 7-1 through 7-4 detail examples of invalid certificates:
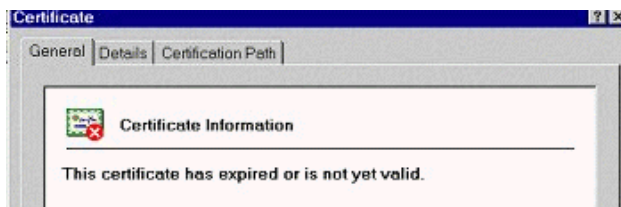
Figure 7-1
Expired Certificate

Figure 7-2
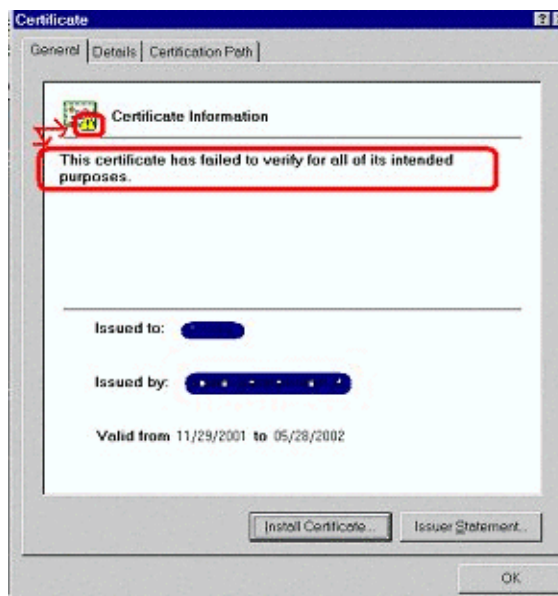Invalid Certificate: Not Intended for EAP-TLS Authentication

Figure 7-3
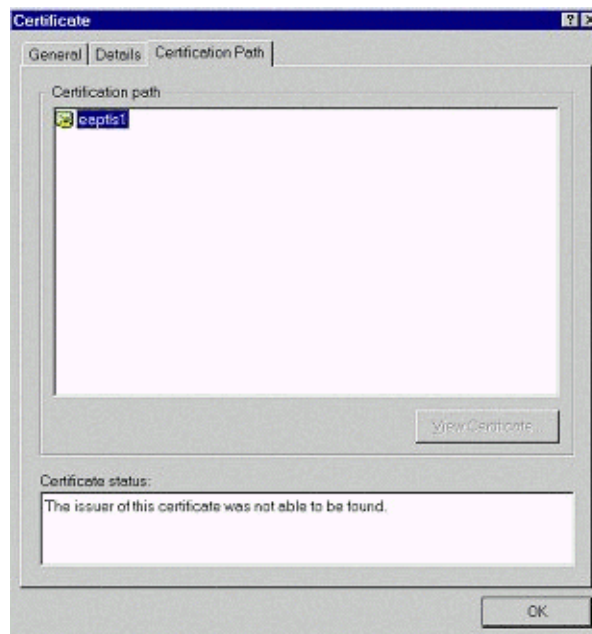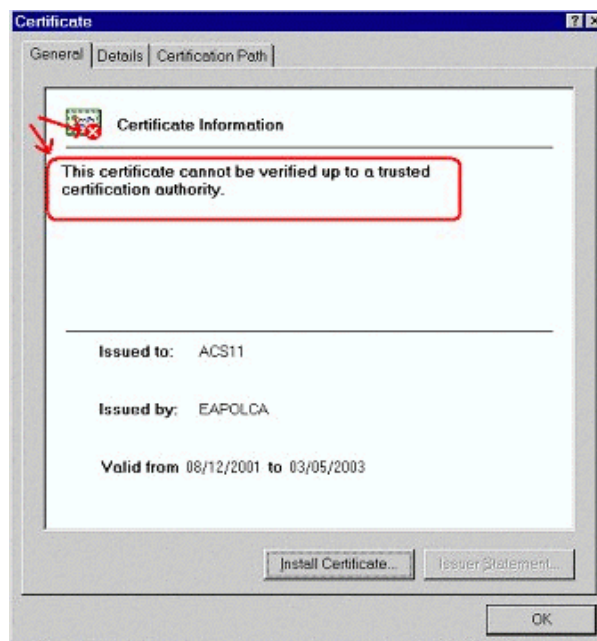Invalid Certificate: Invalid Certification Authority

Figure 7-4
Invalid Certificate: Cannot Verify Root Certification Authority

8 Appendix A—Microsoft Windows 2000 Certificate Services Setup

This appendix provides the procedure used to configure the Microsoft Windows 2000 Server certification authority services in the Validation Lab. Please refer to Microsoft Windows 2000 Server documentation for further help.

Click Add/Remove Programs in the Control Panel and then choose the Add/Remove Windows Components option. Install and configure Certificate Services on the server:

- Select Enterprise Root CA when prompted for the certification authority type.
- Provide the certification authority identifying information.
- Select the default settings for the remaining setup options and allow the Certificate Services installation to complete.
- To set up certificate templates, begin by searching in Windows Help for "CA." From the listed topics, select "Certificate templates," and then under that topic, select the link titled "Establish the certificate types that an enterprise certification authority can issue." Follow the instructions for establishing the certificate type that can be issued, and when prompted select from the template list. Add all certificate templates in the list.
- The instructions for automatic certificate allocation can be found by searching for "auto enrollment" in Windows Help and selecting "Machine certificates for L2TP over IPSec VPN connections" from the list of displayed topics. This topic has a link titled "To configure automatic certificate allocation from an enterprise CA" that provides the necessary setup instructions. During the running of the Automatic Certificate Request Setup Wizard, select Computer or Domain Controller when prompted for a certificate template for certificates to be issued. After the setup wizard has completed the setup, create a computer certificate for the server by typing the following command at the Windows 2000 Server command prompt:

  secedit /refreshpolicy machine_policy

8 Appendix B—Demo Certificates

Sample certificates are provided in the .zip file located at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/tcert.zip, to do EAP-TLS testing (without having to set up the certification authority server infrastructure):

- Three client certificates:
  - eaptls1.p12
  - eaptls2.p12
  - eaptls3.p12
- One server certificate for the AAA server (Windows-based) and one corresponding private key file
  - server.cer (certificate)
  - server.pvk (private key file). Password is "acsi"
- One certification authority certificate that issued the AAA server and the client certificates
  - ca.cer (certificate)

To use the client certificate:

1. Create a user account on the Microsoft XP client (with user-id eaptls1, eaptls2, or eaptls3).
2. Copy the appropriate client certificate to the XP machine and click it to install (private key is inside and does not require a password).
3. Follow instructions in Section 6.4 to complete the Microsoft XP client configuration.

To use the AAA server (Windows-based) and the certification authority certificates:

1. Copy the server certificate, private key file, and the certification authority certificate to the AAA server machine.

2. Install the server certificate and the private key.

3. Install the certification authority server certificate onto the AAA server.

4. Create user accounts for eaptls1, eaptls2, and eaptls3 on the internal AAA server database.

Instructions for installing the server and certification authority certificates onto ACS v3.0:

1. Server certificate installation: From the ACS main menu page, select System Configuration >> ACS certificate setup.

2. Certification authority server certificate installation: From the ACS main menu page select System Configuration >> Certification Authority Setup.

Figure 9-1

Step 1: Server Certificate Installation
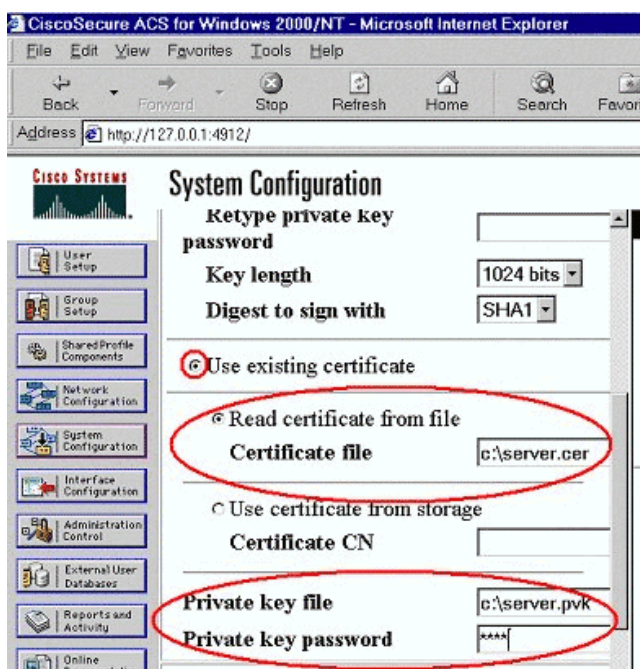
After submitting, you should see the following (no need to restart ACS before you configure the certification authority and enable EAP-TLS):
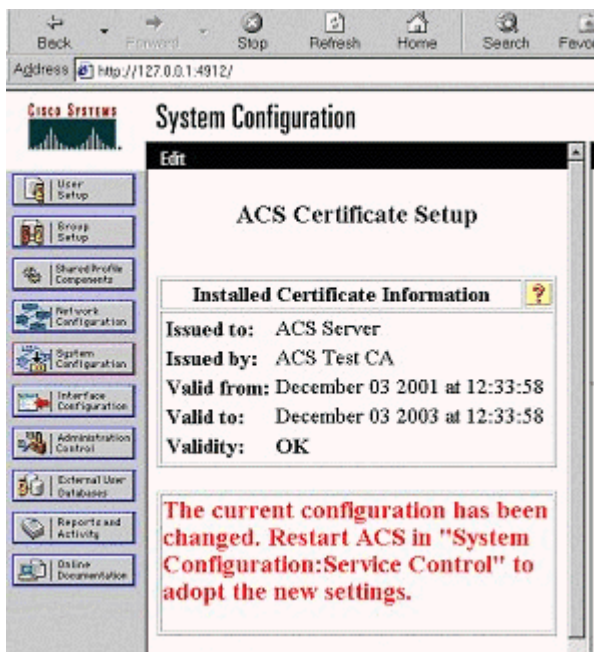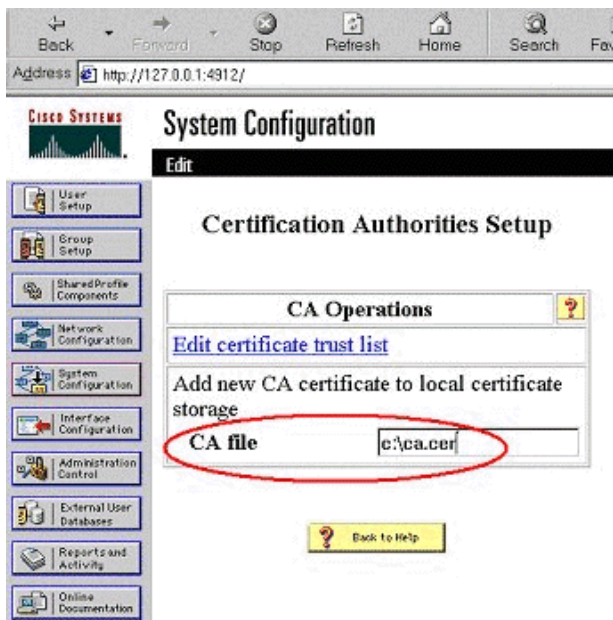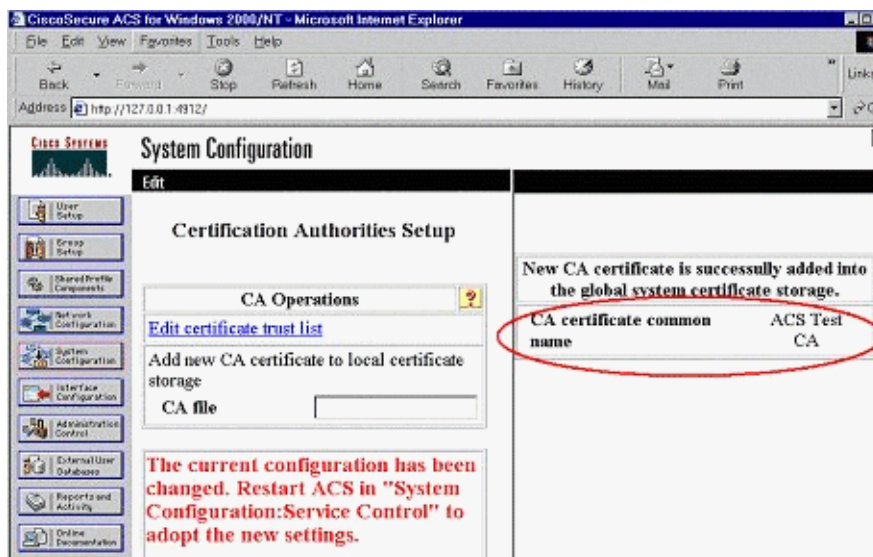

Figure 9-2

Step 2: Certification Authority Server Certificate Installation

Details of the installed certification authority can be seen in the right side of the screen as shown in Figure 9-3 (you do not need to restart ACS before you enable EAP-TLS):

Figure 9-3

Certification Authority Detail Display

As the final step, enable EAP-TLS in the ACS "Global Authentication Setup" and submit and restart the ACS. (Refer to sections 6.2.2 and 6.2.3 for more Details.)

CISCO SYSTEMS

Corporate Headquarters	European Headquarters	Americas Headquarters	Asia Pacific Headquarters
Cisco Systems, Inc.	Cisco Systems Europe	Cisco Systems, Inc.	Cisco Systems, Inc.
170 West Tasman Drive	11 Rue Camille Desmoulins	170 West Tasman Drive	Capital Tower
San Jose, CA 95134-1706	92782 Issy-les-Moulineaux	San Jose, CA 95134-1706	168 Robinson Road
USA	Cedex 9	USA	#22-01 to #29-01
www.cisco.com	France	www.cisco.com	Singapore 068912
Tel: 408 526-4000	www-europe.cisco.com	Tel: 408 526-7660	www.cisco.com
800 553-NETS (6387)	Tel: 33 1 58 04 60 00	Fax: 408 527-0883	Tel: +65 317 7777
Fax: 408 526-4100	Fax: 33 1 58 04 61 00		Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe